Department of Homeland Security Daily Open Source Infrastructure Report for 31 January 2007

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports an explosion leveled a gas station near a ski resort in West Virginia killing at least four people and seriously injuring at least nine others; a propane tank exploded just as a fire truck was pulling into the station in response to reports of a leak. (See item 2)
- A Vermont state computer containing personal information such as names, Social Security numbers, and bank account information for 70,000 Vermonters has been hacked in an automated computer attack that puts their personal information at risk for misuse. (See item 7)
- United Press International reports federal authorities are treating Super Bowl XLI in Miami on Sunday, February 4, as a Level 1 security event with measures far beyond other football games. (See item 39)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *January 30, Associated Press* — **Congress scrutinizing LANL security.** Lawmakers planned to call Tuesday, January 30, for a comprehensive audit of Los Alamos National Laboratory

(LANL) in hopes of discovering why security breaches continue even after tens of millions of dollars have been spent on improvements. Representative Bart Stupak (D−MI) said he wants to evaluate whether the footprint and mission of Los Alamos are too large and whether many of its classified operations should be moved to another lab. At issue are security breaches −− the latest occurring in October −− and a long line of problems at the nuclear−weapons research lab. A new management team was installed at the lab less than a year ago in part to reverse years of security and safety problems. Lawmakers also want to know what has happened to repeated efforts to make the lab disk−less so classified material could no longer be lost or stolen. The rash of security problems at the lab dates back to the late 1990s. It includes the disappearance of two hard drives containing classified material that later were found behind a copying machine and the disappearance of two computer disks that forced a virtual shutdown of Los Alamos. It later was learned the two disks never existed.
Source: http://www.freenewmexican.com/news/56133.html

2. *January 30, Associated Press* — **At least four dead in blast at West Virginia gas station.** An explosion leveled a gas station near a ski resort in West Virginia Tuesday morning, January 29, killing at least four people and seriously injuring at least nine others. Authorities suspect that a propane tank exploded at The Flat Top Little General Store on Route 19, about 10:45 a.m., EST, just as a fire truck was pulling into the station in response to a report of a leak. The cause of the explosion has not been determined. Kim O'Brien, spokesperson for the state Fire Marshal's office, said she's not sure whether it was a propane tank or a liquid petroleum tank that exploded. The explosion was felt at least a mile away.
Source: http://www.cnn.com/2007/US/01/30/gas.station.blast.ap/index. html

3. *January 29, Associated Press* — **NRC says plant operators are not liable for airliner attacks.** The Nuclear Regulatory Commission (NRC) said Monday, January 29, that nuclear power plant operators should not be expected to stop terrorists from crashing an airliner into a reactor, saying that responsibility lies elsewhere. Plant operators instead should focus on limiting radioactive releases and public exposure from any such airborne attack, the agency said in a revised defense plan for America's nuclear plants. Details of the new defense plan are secret. The NRC, in a summary of the security plan, said that "active protection" against an airborne threat rests with organizations such as the Federal Aviation Administration and the military. It said that various mitigation strategies required of plant operators "are sufficient to ensure adequate protection of the public health and safety" in case of an airborne attack. The new plan spells out what the operators of the nation's commercial nuclear power plants must be capable of defending against. It assumes that a terrorist attack force would be relatively small −− and that its weapons would be limited.
NRC statement on final rule amending security requirements:
http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=070290172:2
Source: http://www.foxnews.com/story/0,2933,248221,00.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

4. *January 30, Government Accountability Office* — **GAO−07−397T: Military Personnel: DoD Needs to Provide a Better Link between Its Defense Strategy and Military Personnel Requirements (Testimony).** The war in Iraq along with other overseas operations have led to significant stress on U.S. ground forces and raised questions about whether those forces are appropriately sized and structured. The Office of the Secretary of Defense (OSD) concluded in its 2006 Quadrennial Defense Review that the number of active personnel in the Army and Marine Corps should not change. However, the Secretary of Defense recently announced plans to increase these services' active end strength by 92,000 troops. Given the long−term costs associated with this increase, it is important that Congress understand how the Department of Defense (DoD) determines military personnel requirements and the extent of its analysis. GAO has issued a number of reports on DoD's force structure and the impact of ongoing operations on military personnel, equipment, training, and related funding. This statement, which draws on that prior work, focuses on (1) the processes and analyses OSD and the services use to assess force structure and military personnel levels; (2) the extent to which the services' requirements analyses reflect new demands as a result of the changed security environment; and (3) the extent of information DoD has provided to Congress to support requests for military personnel.
Highlights: http://www.gao.gov/highlights/d07397thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−397T

5. *January 29, Federal Computer Week* — **Cross−domain solutions needed in Iraq.** In Iraq, coalition countries' use of different computer systems to store and share information has led to the "sneaker net," where people must use their feet to share information. Now, the Department of Defense (DoD) is tackling the problem of multinational information sharing from technical, political and cultural standpoints. Officials say cross−domain solutions are needed. "As we see in the theater, interagency and coalition partners all have a problem with information sharing," DoD Chief Information Officer John Grimes said at last week's Network Centric Warfare conference in Washington, DC. "Some of that is in cross−domain solutions, which we're working very hard." Information assurance is the main challenge to fielding technical solutions to the cross−domain problem, Grimes said. "The problem is cross−domain solutions keep popping up [in Iraq] and they've never been certified from an [information assurance] standpoint, so you don't know if there are holes in it."
Source: http://www.fcw.com/article97504−01−29−07−Web

6. *January 29, GovExec* — **Navy developing massive information network.** Department of the Navy officials are in the early stages of developing a massive information network that will encompass all existing department networks including the much maligned Navy−Marine Corps Intranet. Implementation of the Next Generation Enterprise Network, known as NGEN, is scheduled to start in 2010. The network will either subsume or be compatible with all existing Navy networks. The new network's desired capabilities and potential enhancements to existing networks are still being worked out, Navy officials said. The network will be compatible with the Global Information Grid, an all−encompassing Department of Defense communications project that is still in development, and will make use of the Defense Information Systems Agency's Net−Centric Enterprise Services program. According to the Navy, the Center for

Naval Analyses is working to quickly identify the overarching capabilities needed from the network in the 2010 to 2020 timeframe and recommend workable solutions.
Source: http://www.govexec.com/story_page.cfm?articleid=35978&dcn=to daysnews

[Return to top]

Banking and Finance Sector

7. *January 30, Associated Press* — **Personal information on state computer compromised.** A Vermont state computer containing personal information about 70,000 Vermonters has been hacked into in an automated computer attack that puts their personal information at risk for misuse. Human Services Secretary Cynthia LaWare says there's no indication that any of the names, Social Security numbers, or bank account information stored on the computer have been misused. The Human Services computer, which was used to track non−custodial parents who owe back child support, was removed from service after the attack was discovered last month. The incident is the third in recent months that state officials have had to answer for computer−related security breaches.
Source: http://www.wcax.com/global/story.asp?s=6005817

8. *January 30, Websense Security Labs* — **Malicious Website: Vivio Lure spreading crimeware.** Websense Security Labs has discovered a new information−stealing, malicious code attack, which appears to provide more evidence that Russian−based malicious code writers and Brazilians are either working together, or are sharing tools or information. If users click on the link within the e−mail, they are redirected to a page that is hosted in Russia. That page attempts to exploit the user with the "VML" vulnerability. If the user's PC has not been properly patched, the site downloads and runs an executable called "stylecss.exe". This file is packed with "Yoda's protector," and has an MD5 of b6b2ccb8d1b862fa92c71a17c1795af2. The file adds information to the Run key in the registry: (C:\Arquivos de programas\ExAlien.exe). Once running, the file is designed to steal information from end−users when they visit banking Websites.
Source: http://www.websensesecuritylabs.com/alerts/

9. *January 29, IDG News Service* — **Microsoft targets phishers; new browser security technology is in the works.** Microsoft and industry partners are pushing plans to roll out a new technology to combat phishing. At February's RSA security conference in San Francisco, the software giant plans to announce that a number of Websites have gone through a new certification process designed to make it harder for phishers to spoof them. The process gives third−party certification authorities like VeriSign and Entrust a more stringent set of guidelines to follow when they are authenticating Websites. The result of the process is called an Extended Validation Secure Sockets Layer (EV SSL) certificate, which can be used by Websites to help reassure Web surfers that they are handing over their private information to a legitimate site. Sites that have been EV SSL−certified will look a little different from today's secure sites, which typically display a small "lock" icon in the Web browser. When IE hits part of a Website that supports the EV SSL standard, the lock icon will still show but the address bar will also turn green. Users will also be able to see what country the Website is based in and who has certified it. VeriSign has been offering EV SSL certificates since December 11.
Source: http://www.pcworld.com/printable/article/id,128674/printable .html

10. *January 29, Finextra (UK)* — **Hbos bank sends customer 75,000 statements.** UK bank Hbos is investigating how a customer who requested a copy of her bank statement ended up being sent the confidential details of 75,000 other account holders. An inquiry has been launched after Stephanie McLaughlin asked Hbos for a bank statement but received five packages containing 2,500 sheets containing other customers names, sort codes, and account details instead. According to press reports, each page had details for 30 accounts, including pay−in and withdrawal information. Hbos has apologised for the incident, which it says is "serious" but "isolated".
Source: http://finextra.com/fullstory.asp?id=16437

11. *January 29, Finance News Online (UK)* — **Britons warned over ATM practices.** UK payments association Apacs has issued advice regarding cash machine safety in light of the latest crime figures revealing an increase in personal theft. Such crimes rose by 14 percent over the last quarter, the most recent British Crime Survey has shown, with Apacs suggesting that safer practices at cash machines could lower potential risk. Apacs suggests avoiding removing skimming devices, and to instead advise consumers to inform the police or bank. Apacs says that a growing number of initiatives are being trialed, including the use of specially demarcated privacy spaces. "While a zoned area around a cash machine may not seem like much of a deterrent, the research speaks volumes," said Apacs director of communications Sandra Quinn. "...These marked−out areas are a visual reminder to the cash machine user to be vigilant and a clear sign for others to respect the privacy of the person in the space," Quinn continued.
Source: http://www.financenewsonline.co.uk/articles/Britons−warned−over−ATM−practices−18045121.html

12. *January 29, Agence France−Press* — **Bank of America fined for lax money laundering controls.** The NASD securities watchdog said it had fined Bank of America Investment Services, Inc. $3 million for failing to comply with U.S. government anti−money laundering laws. NASD spokesperson Herb Perone said the fine was the largest ever to be levied against a broker−dealer under U.S. anti−money laundering rules. The fine related to offshore accounts held on the Isle of Man, a well−known tax haven. The industry regulator said Bank of America Investment Services (BAI) had "failed to obtain required additional customer information" with regard to 34 accounts. Between $79 million and $93 million dollars were held in the offshore accounts from which multi−million dollar wire transfers were made across international boundaries in recent years. The NASD said BAI allowed the account holders to engage in "multi−million dollar wire transactions" even though it did not have complete ownership details for the accounts, and despite a senior BAI lawyer urging the identification of the accounts' beneficial owners.
Source: http://news.yahoo.com/s/afp/20070129/ts_alt_afp/uscompanybankofamerica_070129204552

[Return to top]

Transportation and Border Security Sector

13. *January 30, Government Accountability Office* — **GAO−07−390T: Rail Safety: The Federal Railroad Administration Is Better Targeting Its Oversight, but Needs to Assess the**

Impact of Its Efforts (Testimony). Although the overall safety record of the railroad industry, as measured by the number of train accidents per million miles traveled, has improved markedly since 1980, there has been little or no overall improvement over the past decade. Serious accidents resulting in injuries and deaths continue to occur, such as one in Graniteville, SC, that resulted in 9 deaths and 292 injuries. The Federal Railroad Administration (FRA) develops safety standards and inspects and enforces railroads' compliance with these standards. On January 26, 2007, the Government Accountability Office (GAO) reported on FRA's overall safety oversight strategy. (See GAO−07−149.) The report discussed how FRA (1) focuses its efforts on the highest priority risks related to train accidents in planning its oversight, (2) identifies safety problems on railroad systems in carrying out its oversight, and (3) assesses the impact of its oversight efforts on safety. GAO recommended that FRA (1) put into place measures of the results of its inspection and enforcement programs and (2) evaluate its enforcement program. In reviewing a draft of that report, the Department of Transportation did not provide overall views on its contents or its recommendations. The statement is based on GAO's recent report.
Highlights: http://www.gao.gov/highlights/d07390thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−390T

14. *January 30, Federal Aviation Administration* — **FAA to propose pilot retirement age change.** Federal Aviation Administration (FAA) Administrator Marion C. Blakey on Tuesday, January 30, announced that the FAA will propose to raise the mandatory retirement age for U.S. commercial pilots from 60 to 65. Speaking before pilots and aviation experts at the National Press Club, Blakey said that the agency plans to propose adopting the new International Civil Aviation Organization (ICAO) standard that allows one pilot to be up to age 65 provided the other pilot is under age 60. The FAA plans to issue a formal Notice of Proposed Rulemaking later this year and will publish a final rule after careful consideration of all public comments. On September 27, 2006, Administrator Blakey established a group of airline, labor and medical experts to recommend whether the United States should adopt the new ICAO standard and determine what actions would be necessary if the FAA were to change its rule. Since 1959, the FAA has required that all U.S. pilots stop flying commercial airplanes at age 60. In November 2006, ICAO, the United Nations' aviation organization, increased the upper age limit for pilots to age 65, provided that the other pilot is under age 60.
The November 29, 2006 Age 60 ARC report, appendices, and public comments are available online at http://dms.dot.gov/ docket number 26139.
Source: http://www.faa.gov/news/press_releases/news_story.cfm?newsId =8027

15. *January 30, Reuters* — **Air travelers seen doubling by 2025.** The number of air travelers is expected to double by 2025, rising to more than nine billion a year, a body representing the world's airports said on Tuesday, January 30. The Airports Council International (ACI) predicted air freight would triple over the same period. In its Global Traffic Forecast 2006−2025, ACI said passengers passing through the 1,650 domestic and international airports its 567 members operate would grow an average four percent annually over the period. There are currently around 4.2 billion air travelers a year. Environmentalists say aviation is a growing source of carbon dioxide which contributes to global warming. By 2025, Asia will be challenging North America, which has held the top spot as the busiest global air passenger region since the dawn of civil aviation.
Source: http://www.usatoday.com/travel/news/2007−01−30−air−travelers

−to−double−2025_x.htm

16. *January 30, Choctaw Sun (AL)* — **Railroad officials think vandals caused Alabama train derailment.** A freight train parked at the Concord Road crossing on the Meridian and Bigbee's line in Yantley, AL, unexpectedly began to move in the predawn hours Sunday, January 28, rolling more than a mile and a half down the tracks where it collided with another set of parked rail cars across County Road 1 near the intersection of Watermelon Drive. An M&B spokesperson in Meridian told the Choctaw Sun on Monday that because the brakes were properly set on the train, the company suspects foul play. An investigation involving the Federal Railroad Administration and other agencies was ongoing Monday afternoon. The two−engine train was pulling about 97 cars, according to Bill Gibson, Director of Choctaw County's Emergency Management Agency. Several boxcars loaded with new kitchen appliances sustained heavy damage, Gibson said. M&B Railroad is owned by Genessee and Wyoming, Inc., a provider of rail−freight transportation and its supporting services in the United States, Canada, Mexico, South America, and Australia.
Source: http://www.meridianstar.com/local/local_story_030001902.html

17. *January 30, Associated Press* — **Airlines face higher baggage liability.** U.S. airlines' liability for lost or damaged luggage will soon increase to $3,000 per passenger from the current limit of $2,800 under a rule issued by the Department of Transportation Monday, January 29. This will take effect February 28, 2007 Airlines could pay an additional $2.6 million per year to passengers as a result of the new regulation, the department estimated. Under the department's rules, airlines cannot limit their liability to less than $2,800 for losing or damaging passengers' luggage. Passengers can buy additional insurance if they believe their luggage is more valuable than that. The department did not name specific airlines but said it would apply to any flight using "large aircraft" and said that only small air taxis and commuter air carriers are exempt from the rule.
Source: http://biz.yahoo.com/ap/070129/airlines_baggage_liability.ht ml?.v=1

18. *January 30, Inside Bay Area (CA)* — **Police: More than one shooter in Hayward BART incident?** Multiple shooters may have been involved in a gunfight outside the Hayward BART station Monday evening, January 29, that left four people injured, including an AC Transit bus driver, Bay Area Rapid Transit (BART) spokesperson Linton Johnson said on Tuesday, January 30. No motive has been established for the shooting, but police are questioning one suspect in custody, Linton said. The shooting, which was reported at 5:48 p.m. PST Monday, closed the downtown Hayward BART station for nearly two hours as police investigated the incident.
Source: http://www.insidebayarea.com/timesstar/ci_5118614

19. *January 29, Reuters* — **EU wants to keep limits on U.S. passenger data use.** The European Commission (EU) wants to retain existing limits on how the United States uses data on incoming air passengers despite U.S. calls for more flexibility, a spokesperson said on Monday, January 29. Under a temporary deal reached in October as part of U.S. efforts to combat terrorism, European airlines must pass on up to 34 items of data, including passengers' addresses and credit card details, to be allowed to land at U.S. airports. U.S. Department of Homeland Security Secretary Michael Chertoff said last week that Washington would not look for more data in forthcoming negotiations on a permanent accord but would push for more flexibility in how it could use the information. The United States has also been pushing for the

right to hold data on passengers for longer.
Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyID=2007−01−29T185101Z_01_L29247463_RTRUKOC_0_US−AIRLINES−EU−USA.xml&WTmodLoc=USNewsHome_C2_domesticNews−5

20. *January 29, KETV (NE)* — **Eppley Airfield scare over powder.** Passengers allowed off a United Airlines flight from Denver that was being held at the end of a runway at Eppley Airfield in Omaha, NE, on Monday afternoon, January 29, said they think a sugar substitute is to blame. The head of the Airport Authority, Don Smithey, told KETV NewsWatch 7 that a hazardous materials crew entered the United jet at about 12:30 p.m. CST Monday. At about 2:45 p.m., the plane was moved off the tarmac. A KETV crew at the scene said Omaha Fire Department, Omaha Police Department, Airport Authority and Hazmat crews surrounded the plane. A United representative said a crewmember noticed a powder in the galley at the rear of the plane.
Source: http://www.ketv.com/news/10871793/detail.html?subid=22100461&qs=1;bp=t

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

21. *January 30, Agricultural Research Service* — **DNA fingerprinting.** Identifying individual animals is essential to controlling diseases and monitoring international imports and exports. To find out who's who in a herd, scientists and cattle industry professionals rely on DNA −−especially when traditional animal identification has been lost or damaged. Highly specialized genetic markers, developed by Agricultural Research Service (ARS) scientists at the U.S. Meat Animal Research Center (USMARC), Clay Center, NE, are helping to improve animal identification and parentage testing. The most common type of genetic marker present in U.S. beef and dairy cattle is the single nucleotide polymorphism (SNP). The scientists have already identified 122 specialized parentage SNPs and annotated more than 1,600 neighboring SNPs. This knowledge has increased the accuracy of parentage and identification tests. Using genetic markers, scientists can generate molecular fingerprints to match multiple samples from one animal. DNA−based technology is an effective complement to physical markers—such as brands, tattoos, tags and implants—and can clearly identify animals in situations in which physical markers cannot. DNA can be obtained and analyzed from cattle at any stage of life, as well as from fresh, frozen or cooked products. It's stable and completely unique to each animal. Since 2003, USMARC researchers have identified over 7,000 bovine SNPs and placed them in the public domain.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

22. *January 29, Dow Jones* — **Two Brazil states close Bolivia border for animal safety.** Two of Brazil’s major cattle−ranching states have prohibited transit of live animals and farm goods

from Bolivia following an outbreak of foot−and−mouth disease in that neighboring country. The Mato Grosso state government said in a statement on Monday, January 29, that agriculture officials were discussing other preventative measures. Mato Grosso do Sul will close its border with Bolivia, the local Estado newswire reported. In October 2005, a series of foot−and−mouth cases were reported on the Paraguay border with Mato Grosso do Sul, leading ranchers in the state to charge that Paraguay cattle had crossed the border and infected the Brazilian herd. “Luckily our border with Bolivia is not as porous as our border with Paraguay. Cattle have to cross the Paraguay River if they want to get into the state,“ Ademar Silvia, president of the Mato Grosso do Sul Agriculture Federation, told Dow Jones Newswires. Bolivia’s government reported foot−and−mouth disease on Sunday in Santa Cruz, some 300 miles from the border of Mato Grosso do Sul.
Source: http://www.cattlenetwork.com/content.asp?contentid=101527

23. *January 29, Pennsylvania State University* — **Honeybee die−off alarms keepers, growers and researchers.** An alarming die−off of honeybees has beekeepers fighting for commercial survival and crop growers wondering whether bees will be available to pollinate their crops this spring and summer. Researchers are scrambling to find answers to what's causing an affliction recently named Colony Collapse Disorder, which has decimated commercial beekeeping operations in Pennsylvania and across the country. "During the last three months of 2006, we began to receive reports from commercial beekeepers of an alarming number of honeybee colonies dying in the eastern U.S.," said Maryann Frazier, apiculture extension associate in Penn State's College of Agricultural Sciences. "Since the beginning of the year, beekeepers from all over the country have been reporting unprecedented losses. "This has become a highly significant yet poorly understood problem that threatens the pollination industry and the production of commercial honey in the U.S.," she said. "Because the number of managed honeybee colonies is less than half of what it was 25 years ago, states such as Pennsylvania can ill afford these heavy losses." A working group of university faculty researchers, state regulatory officials, cooperative extension educators and industry representatives is working to identify the cause of Colony Collapse Disorder and to develop management strategies and recommendations for beekeepers.
Source: http://live.psu.edu/story/21979

[Return to top]

Food Sector

24. *January 29, Food Safety and Inspection Service* — **Ground beef products recalled.** The Natural State Meat Co., a Batesville, AR, firm, is voluntarily recalling approximately 4,240 pounds of ground beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) announced Monday, January 29. The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of these products. The ground beef products were produced on various dates between January 19 and 26, 2007 and were distributed to retail establishments and institutions in Independence County, AR. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_008_2007_Relea se/index.asp

[Return to top]

Water Sector

25. *January 30, Arizona Daily Star* — **Police water accidentally polluted at headquarters.** A garden hose mistakenly connected to a hot−water boiler pumped tainted water into Tucson, AZ, Police Department headquarters, preventing the police from using the building's water fountains, sinks and showers since Friday, January 26. No police officers drank or showered with the "black water," said Assistant Chief Sharon Allen, and city officials believe there was no wider contamination of the drinking water for the surrounding neighborhoods. The Pima County Health Department assessed the building after the water lines had been flushed and sent the city a letter Monday, January 29, saying there was "no reason to restrict the use of the internal water system."
Source: http://www.azstarnet.com/metro/166808

[Return to top]

Public Health Sector

26. *January 30, Reuters* — **China meeting warns of bird flu mutation risk.** The H5N1 strain of the bird flu virus is rapidly mutating and the world must be on guard even though the disease has yet to be transmitted between humans, experts told a meeting in Beijing, Chinese media said on Tuesday, January 30. The closed door conference, attended by experts from the Chinese and U.S. centers for disease control and the World Health Organization among others, opened on Monday, January 29, the official newspaper of the Chinese Health Ministry reported. "The experts said that despite there being no evidence yet of human−to−human transmission of bird flu, the highly pathogenic H5N1 form of the virus is continuing to rapidly mutate, and human infections keep happening," the Health News reported. The report provided no other details, except that the meeting will discuss bird flu vaccines.
Source: http://today.reuters.com/News/CrisesArticle.aspx?storyId=PEK200089&WTmodLoc=IntNewsHome_C4_Crises−6

27. *January 29, Reuters* — **New technique can identify counterfeit drugs.** A new method of verifying the ingredients of a pharmaceutical product without opening the package is more accurate than the conventional methods of analysis, scientists in the United Kingdom report in a study scheduled for publication March 1. Spatially offset Raman spectroscopy (SORS) can probe deep layers of material, separating out interfering signals emanating from packaging, drug coatings, and inactive ingredients. In that way, SORS authenticates the actual content and concentration of a drug, Pavel Matousek and Charlotte Eliasson of the Rutherford Appleton Laboratory in Oxfordshire report. It can do so without ever having to open a package, they say. Sometimes a product has the correct molecule, but its altered formulation may decrease its effectiveness or the concentration may be wrong. Other times, the product may have none of the ingredients that it claims to contain. But if a package has to be opened to verify its contents, it can no longer be marketed.
Source: http://today.reuters.com/news/articlenews.aspx?type=scienceN

ews&storyID=2007−01−30T013205Z_01_TON005499_RTRUKOC_0_US−COUNTERFEIT−DRUGS.xml&WTmodLoc=SciNewsHome_C2_scienceNews−6

28. *January 29, Agence France−Presse* — **Russia registers new outbreak of bird flu.** Russia has registered its first cases of H5N1 bird flu since an outbreak hit dozens of towns and villages last year, Russian media reported. "A laboratory analysis uncovered the H5N1 bird flu virus," in poultry at three locations in the southern Krasnodar region, said Aleksei Alekseyenko, an official at the country's agricultural inspection agency Rosselkhoznadzor, the RIA Novosti news agency reported. The three infected areas are located near the country's Black Sea coast. Bird flu was discovered at over 90 points in southern Russia and Siberia in 2006, with the last quarantine lifted in August.
Source: http://news.yahoo.com/s/afp/20070130/hl_afp/healthflurussia_070130001020;_ylt=Ao2AWLhHKvrrxSXLrSSKMn2JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

29. *January 29, Reuters* — **Court order keeps Canadian tuberculosis patient in hospital.** Canadian health officials have won a court order to keep a patient with a new, highly drug−resistant strain of tuberculosis in hospital, while the national health agency says it will start tracking rates of the disease this year. Health officials in Toronto say the person has been confined to treatment for 11 months. "Basically, this is someone who dropped in and out of treatment over a number of years," Elizabeth Rae, associate medical officer of health with the tuberculosis program at Toronto Public Health, said on Monday, January 29. A court order was considered necessary given the person's history of sporadic care, Rae said. Although not currently infectious, the patient will likely stay in hospital under strict watch for another year. Officials are monitoring a second person who had the strain, which is dangerous because conventional drugs don't work to contain it.
Source: http://www.alertnet.org/thenews/newsdesk/N29190909.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *January 31, Government Accountability Office* — **GAO−07−60: Actions Needed to Identify National Guard Domestic Equipment Requirements and Readiness (Report).** The high use of the National Guard for federal overseas missions has reduced equipment available for its state−led domestic missions, at the same time it faces an expanded array of threats at home. The massive state−led, federally funded response to Hurricane Katrina illustrates the Guard’s important role in responding to the effects of large−scale, multistate events as well as the difficulty of working with multiple state and federal agencies. To address congressional interest in the Guard’s domestic preparedness, GAO assessed the extent to which (1) the Guard’s domestic equipment requirements have been identified, (2) the Department of Defense (DOD)

measures and reports to Congress the equipment readiness of non−deployed Guard forces for domestic missions, and (3) DOD actions address the Guard's domestic equipping challenges. GAO examined the National Guard's plans and equipment status and included case studies in California, Florida, New Jersey, and West Virginia. GAO recommends updating the National Guard Bureau's charter and civil support regulation and improved reporting of the Guard's domestic readiness. DOD partially agreed to report on plans to assess domestic readiness but disagreed with other recommendations. GAO reiterates the need for changes in matters for congressional consideration.
Highlights: http://www.gao.gov/highlights/d0760high.pdf
Source: http://www.gao.gov/docsearch/abstract.php?rptno=GAO−07−60

31. *January 30,* — **States push earthquake awareness.** The U.S. Geological Survey says the central U.S. has more earthquakes than any other part of the country east of the Rocky Mountains. With that in mind, emergency planners and responders want the public to be ready. Arkansas, Mississippi, western Tennessee and Missouri, are holding Earthquake Awareness Weeks to coincide with the anniversary of the third of three devastating 1811 to 1812 Seismic Zone earthquakes in New Madrid, MO−−magnitude 8 quakes that struck in December, January and February. The quakes are said to have been the strongest earthquakes to ever hit the U.S. "It made sense to coordinate (the awareness week) with the February 7 historic earthquake," said Steve Oglesby, the earthquake program manager for the Kentucky Division of Emergency Management (KDEM). The consolidation of the awareness weeks was a move pushed by the Central United States Earthquake Consortium, of which the states are all members. Each state will hold events geared toward the public, schools, businesses and the government.
Source: http://www.disasternews.net/news/news.php?articleid=3438

32. *January 30, Eufaula Tribune (AL)* — **Hazardous alert sirens to be tested.** Officials in Barbour County, AL, recently installed new warning systems in several areas in Barbour County. The town of Eufaula is now being served by a new severe weather and hazardous material (Hazmat) alert system in the Eufaula Industrial Park. The new siren is different from others in the county in that it can also be used to warn people in the surrounding areas in the case of a chemical spill at one of the nearby plants. "Officials can also talk through the system from the E−911 office to let people know what they need to do in case of a chemical spill," Barbour County Homeland Security Director Ronnie Dollar says. All of the warning systems in the county will be tested on Wednesday, February 7, at noon if weather permits. Citizens should expect to hear the sirens and also a voice advising people of a Hazmat situation.
Source: http://www.zwire.com/site/news.cfm?newsid=17782246&BRD=2235&PAG=461&dept_id=439676&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

33. *January 30, Sophos* — **Korean programmers arrested for sending 1.6 billion spam e−mails.** Sophos has welcomed the arrests of two men suspected of being involved in one of South Korea's biggest spam incidents. The men, one aged 20 and the other 26−years−old, are alleged to have broken the law by sending out 1.6 billion spam e−mails between September and December 2006. South Korean authorities in Seoul claim that the duo, both computer

programmers, obtained personal and financial information from 12,000 victims which they then sold to other firms. South Korea was revealed in Sophos' recent security report as the third−worst nation in the world for relaying spam.
Source: http://www.sophos.com/pressoffice/news/articles/2007/01/kore anspam.html

34. *January 30, IDG News Service* — **Cingular, Priceline, Travelocity settle adware suit.** Cingular Wireless, Priceline.com, and Travelocity.com have settled with New York State's attorney general after the state accused them of contributing to the spread of adware. The companies agreed to pay fines and take steps to help keep adware off users' PCs but did not admit guilt in the case. It marked the first time law enforcement had held advertisers responsible for ads delivered via adware, according to a statement by Attorney General Andrew Cuomo's office. DirectRevenue actually installed the adware.
Source: http://www.infoworld.com/article/07/01/30/HNcingularpricelin etravelocity_1.html

35. *January 30, CNET News* — **Experts: Don't buy Vista for the security.** Windows Vista is a leap forward in terms of security, but few people who know the operating system say the advances are enough to justify an upgrade. Microsoft officially launched Vista for consumers Tuesday, January 30. The software giant promotes the new operating system as the most secure version of Windows yet. It's a drum Microsoft has been beating for some time. Now that Vista is finally here, pundits praise the security work Microsoft has done. However, most say that is no reason to dump a functioning PC running Windows XP with Service Pack 2 and shell out $200 to upgrade to Vista. "As long as XP users keep their updates current, there's generally no compelling reason to buy into the hype and purchase Vista right away," said David Milman, chief executive of Rescuecom, a computer repair and support company. "Upgrading to Vista is pretty expensive, not only the new software but often new hardware as well," said Gartner analyst John Pescatore. "If you put IE 7 on a Windows XP SP2 PC, along with the usual third−party firewall, antiviral and antispyware tools, you can have a perfectly secure PC if you keep up with the patches."
Source: http://news.com.com/Experts+Dont+buy+Vista+for+the+security/2100−1016_3−6154448.html?tag=nefd.lede

36. *January 30, CNET News* — **Spanish start−up promises free Wi−Fi for all.** A small Spanish start−up called Whisher is thumbing its nose at U.S. broadband providers as it prepares to launch a new service that lets people share their broadband connections via Wi−Fi. "Either you believe in the user−generated revolution or you believe ISPs rule the world," said Ferran Moreno, co−founder and CEO of Whisher. "I believe ISPs don't rule the world and how the Internet works." Of course, there is one small snag in Moreno's utopian view of free Wi−Fi for everyone. In the U.S., it's illegal. Time Warner and other broadband providers such as Verizon Communications said it's rare that they have to take action against subscribers sharing their broadband service outside their home. But representatives from each company said that if illegal sharing persists, the company takes action, which could result in users getting their service cut off or even facing prosecution. So far, broadband providers have not come down hard on other companies proposing to build free Wi−Fi networks that cobble together networks using existing Wi−Fi hot spots. But this could be because these networks are still relatively new, and their service models require additional equipment.
Source: http://news.com.com/Spanish+start−up+Whisher+promises+free+Wi−Fi+for+all/2100−7351_3−6154438.html?tag=nefd.lede

37. *January 30, Information Week* — **Organized malware factories threaten Internet users, study says.** Spam, malware, phishing, and other forms of cyberattacks will likely increase in 2007 as more cyber−criminals organize into sophisticated manufacturing and distribution networks that mirror in structure the computer industry's legitimate production channels, according to a study released Monday, January 29. The study, authored by IBM, warns of the emergence of a so−called "exploits−as−a service" industry. "Managed exploit providers are purchasing exploit code from the underground, encrypting it so that it cannot be pirated, and selling it for top dollar to spam distributors," the report says. The industrialization of malware production will make it tougher for corporate IT security departments to stay ahead of the hackers, says an IBM researcher who helped author the study. "With this whole infrastructure that these criminal organizations are building they can not only target these attacks, they can build custom malware to be used against you. Meaning the probability of you being affected by a piece of malware no one has ever seen before is much higher today than it ever was before," says Gunter Ollmann, director of security strategy at IBM's Security Systems unit.
Report: http://www.iss.net/documents/whitepapers/X_Force_Exec_Brief. pdf
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=JSHY1CJG1SGRIQSNDLRCKHSCJUNN2JVN?articleID=197001739

38. *January 29, CNET News* — **Net pioneer predicts overwhelming botnet surge.** Internet pioneer Vint Cerf has warned high−powered attendees at the World Economic Forum in Davos, Switzerland, that the Internet is at serious risk from botnets. Vast networks of compromised PCs, used by criminals for sending spam and spyware and for launching denial−of−service attacks, are reported to be growing at an alarming rate in terms of their potential. Cerf, now an employee of Google, warned that they could undermine the future of the Internet and likened their spread to a pandemic. Cerf predicted that a quarter of all PCs currently connected to the Internet −− around 150 million −− could be infected by Trojans that covertly seize control of a computer and its broadband connection, handing control of both to criminals in remote locations. According to Mark Sunner, chief security analyst at MessageLabs, Cerf's words of warning are far from scaremongering and the picture is at least as serious as Cerf paints it.
Source: http://news.com.com/Net+pioneer+predicts+overwhelming+botnet+surge/2100−7348_3−6154221.html

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	The top 10 Target Ports are temporarily unavailable. We apologize for the inconvenience. Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

39. *January 30, United Press International* — **Federal agencies involved in Super Bowl.** Federal authorities are treating Super Bowl XLI in Miami on Sunday, February 4, as a Level 1 security event with measures far beyond other football games. Security has included background checks on everyone working at Dolphins Stadium or connected with the event in other ways. More than 30 federal agencies are involved in an effort that includes U.S. Coast Guard patrols of canals and inlets. Sixty bomb−sniffing dogs will also be at work, sweeping the stadium and all other Super Bowl venues, Julie Torres, a spokesperson for the Bureau of Alcohol, Tobacco and Firearms said. About 70,000 people are expected in the stadium Sunday when the Indianapolis Colts and Chicago Bears square off. Thousands more are expected to turn out in South Beach and similar areas to watch the game.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20070130−03442 6−1179r

40. *January 30, Associated Press* — **Robot parking garage to open in New York.** Starting in February, New York's first robotic parking will open in Chinatown. The technology has had a good track record overseas. The developers of the Chinatown garage are counting on the technology to squeeze 67 cars in an apartment−building basement that would otherwise fit only 24; this is accomplished by removing a ramp and maneuver space normally required. The driver stops the car on a pallet and gets out. The pallet is then lowered into the innards of the garage, and transported to a vacant parking space by a computer−controlled contraption similar to an elevator that also runs sideways. Another company had built the only other public robotic garage in the United States. Built in 2002 across the river in Hoboken, NJ, with 314 spaces for monthly rentals only, the garage dropped an unoccupied Cadillac Deville six floors in 2004 and a Jeep four stories the following year. The two loading bays in the Chinatown garage are outfitted with laser and radar sensors that sense if the car fits on the pallet (it's large enough for medium−sized SUVs) and look for movement to determine whether the driver and passenger have left the car.
Source: http://www.wusa9.com/news/news_article.aspx?storyid=55425

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer